REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Amendments to Specification

The specification has been amended by changing "EXOR" to the more conventional –XOR– to indicate the "exclusive OR" operation used to falsify the data.

2. Rejection of Claims 1-18 Under 35 USC §101

This rejection has been addressed by amending claims 1, 22, and 34 to more positively recite the data carrier and method of the invention in terms of structures and method steps. The changes are matters of form only, no new limitations having been added.

It is respectfully noted that:

a. claim 1 positively recites a **data carrier** with a **semi-conductor chip** including a **memory** containing an **operating program**, the operating program being limited to execution of certain types of operating program commands, execution of the commands in way that prevents detection of *data* processed with the corresponding commands based on signals detectable from outside the semiconductor chip;

b. claim 22 positively recites the step of **causing** the data carrier to perform security-relevant operations in one of two specified ways; and

c. claim 34 positively recites the steps of **executing** the plurality of operations, and of **varying** the order of operations.

A data carrier with a semi-conductor chip and memory clearly falls into the statutory category of an apparatus. While claim 1 recites "steps" performed by the operating program, the data carrier is "**arranged**" to perform the steps in question, *i.e.*, the structure of the data carrier, and in particular the operating program included therein, is determined by the steps performed,

which is not inconsistent with the claim of an apparatus. To the contrary, an "**operating program**" can only be defined in terms of its **function**, the "structure" of the program being in the form of circuitry (*i.e.*, hardware) or electric or magnetic charges in a memory (*i.e.*, software). As a result, it is respectfully submitted that claim 1 is a proper apparatus claim, and withdrawal of the rejection of claims 1-21 under 35 USC §101 is respectfully requested.

Claims 22 and 34, on the other hand, have been amended to positively recite the method step(s) of "causing," "executing," and "varying," and therefore clearly fall into the "process" class of 35 USC §101. As a result, withdrawal of the rejection of claims 22-25 and 34-41 under 35 USC §101 is respectfully requested.

2. Rejection of Claims 1-41 Under 35 USC §112, 2nd Paragraph

This rejection is respectfully traversed and/or has been addressed, as follows:

a. Claim 1 has been amended to more positively recite the semiconductor chip, memory, and operating program of the claimed invention. The operating program is properly and necessarily claimed in terms of its function, as is customary in this type of case. As noted above, it is impossible to recite the thousands of integrated circuit elements and/or memory arrangement that makes up the actual "structure" of the data carrier that constitutes the operating program, particular since the same operating program could be implemented using a wide variety of integrated circuit and memory "structures."

b. In answer to the Examiner's questions concerning claims 3 and 34, it is respectfully submitted that while the signal patterns from two different commands might not be identical, the characteristics of the radiation generated by the commands might nevertheless be sufficiently similar, or even identical, as to make it impossible to infer the commands based on analysis of the signal patterns. This is because the commands must be inferred from statistical analysis of the "characteristics" of the radiation during execution of multiple commands. The radiation from any two commands might be

identical or different. It is only over time that individual commands can be inferred from the patterns. By selecting commands that all provide identical or similar radiation patterns or characteristics, it is possible to make it more difficult to infer individual commands from the patterns.

c. In answer to the Examiner's confusion concerning the terms "falsify" and "compensate," the Applicant respectfully submits that these terms in fact do not correspond to "encrypt" and "decrypt." To the contrary, an understanding of these terms is essential to an understanding of the invention. An explanation follows:

c1. Falsification

"Falsification" refers to operations that are applied to the input data ***before*** storage on the card. For example, the input data might be a secret key, which is "falsified" by XORing the secret key with a random number. Without knowing the random number, an attacker cannot infer the secret key from the XORed secret key. Only the XORed secret key is stored on the card and operated upon by the operating program, and therefore the secret key is protected even if an attacker is able to analyze signal patterns and discover the XORed or "falsified" secret key stored on the card, on which the operations are actually performed.

c2. Compensation

The term "compensation," on the other hand, refers to the modified operations that are performed on the falsified data, in order to obtain the same result as if the original operations had been performed on the unfalsified data. Suppose, for example, that the card needs to perform various operations f on a secret key k in order to obtain a result A, *i.e.*, $A = f(k)$. A might, by way of example, be a result used in the authentication of data. As explained above, in order to prevent discovery of the secret key, the secret key is falsified by performing an XOR operation on the key ***before*** it is stored on the card, in order to obtain falsified secret key k'. However, since falsified key k' has been modified,

the result of performing function f on k' would not be A. Instead, the result would be A $\neq f$(k'). In order to obtain A using the falsified data, it is necessary to modify the operations performed on the falsified data to obtain modified operations f', *i.e.*, A=f'(k') where f' are modified versions of f necessary to obtain the result A when f' is performed on falsified data k', *i.e.*, to **compensate** for the changes in k..

It is respectfully submitted that these terms are not at all unclear, but rather represent the most reasonable and clear way to describe the concepts involved. Falsification and compensation are not equivalent to "encryption" and "decryption," and in fact do not generally involve either encryption or decryption. Accordingly, it is respectfully submitted that the proposed substitution of encryption and decryption for falsification and compensation would be inaccurate and unclear, and that the rejection of claims 5, 6, 26, and 27 based on use of the terms falsification and compensation should be withdrawn.

d. The rejection of claim 9, 10, 29, and 30 has been addressed by amending claims 9 and 30 to refer back to the combination "two or more existing auxiliary data" recited in claims 8 and 26, although it is respectfully noted that the words "existing" and "data" already limited the reference to the combination of existing auxiliary data and auxiliary function values in original claims 9 and 29 to the combination of "existing auxiliary data and auxiliary function values" recited claims 8 and 26.

e. The rejections of claims 13, 19, 34 and 40 based on improper use of the word "it" have been addressed by deleting the "it holding" phraseology of claims 13 and 34, and by amending claims 19 and 40 to recite fixing of the next operation to be executed.

f. The rejections of claims 22 and 34 have been addressed, as explained above in connection with the rejection under 35 USC §101, by amending claim 22 and 34 to more explicit recite method "steps."

4. Rejection of Claims 1-4, 13-25, and 34-41 Under 35 USC §102(e) in view of U.S. Patent No. 6,061,449 (Candelore)

This rejection is respectfully traversed on the grounds that the Candelore patent does not disclose or suggest execution of commands in the operating program of a data carrier in such a way that the data processed by the corresponding commands cannot be inferred from signals detectable from outside the semiconductor chip of the data carrier, as recited in **independent claims 1, 22, and 34**, whether by:

a. execution of the commands using byte-by-byte processing of data (as opposed to bit-by-bit processing), as recited in **claims 2 and 23**;

b. choosing commands that generate indistinguishable signal patterns, as recited in claims **3 and 24**,

c. choosing commands that lead to signal patterns which are substantially independent of the data processed, as recited in **claims 4 and 25**; or

d. changing the order of execution of operations, as recited in claims **13-19 and 34-40**.

Instead, the Candelore patent concerns a procedure for "scrambling" encrypted program information and authentication information being communicated from an external storage device to the buffers of a secure circuit, so that the programming sequence of the secure circuit cannot be detected by intercepting the communicated data. This has nothing to do protecting data input operated upon by the operating program of a data carrier semiconductor chip through detection of signals radiated by the chip. Instead, Candelore (in effect) simply hides the order of execution of program steps by the secure circuit by changing the sequence in which the secure circuit retrieves data from the memory. There is no attempt to prevent someone from analyzing the **signals emitted by the secure circuit** of Candelore as opposed to the **sequence of data retrieval from an external memory**.

The claimed invention concerns the problem that internal chip operations can be inferred by statistical analysis of the radiation or electro-magnetic signals emitted by the chip during operation, and in particular the problem that once the program operations are inferred, the secret

data operated upon by the program can be determined based on the chip output. The problem is addressed by more carefully controlling the operating program to make it more difficult to analyze the radiation, by having the program execute commands in bytes, choosing commands based on the radiation generated, varying the order of execution of operations so that the results can be obtained while generating different radiation patterns, and/or doctoring the input data before storage on the data carrier.

Thus, the invention takes the approach that **input** data used by the operating program can be protected by applying the above steps to the operating program. This input data is not scrambled during retrieval from an external memory, as in Candelore, but rather stored on the chip. It might be stored in masked or falsified form, but it is never transmitted from an external memory. The Candelore patent concerns an entirely different problem than the claimed invention. The invention arranges the operating program steps so that the radiation generated cannot be used to determine the steps, whereas the Candelore patent does not concern the **arrangement of the operating program steps**, but merely the **manner in which data is retrieved** from the external memory during execution of the security related operating program.

There is nothing in Candelore to prevent an attacker from analyzing the signals emitted by the chip rather than the data retrieval sequence. No steps are taken to vary execution of the operating program within any particular chip to make the radiation generated thereby, *i.e.*, the claimed "*signals* [caused by a command and] *detectable from outside the semiconductor chip during execution of the command within the semiconductor chip*" more difficult to analyze. Data input is scrambled during execution, but not the manner in which the data is processed. In the method of Candelore, there is no falsifying of input data before execution of the operating program (as opposed to changing the manner of data retrieval from a memory), no varying of program steps, and no suggestion that the program commands be implemented on a byte-by-byte basis. *Retrieving data from a memory in blocks, as in Candelore, is not the same as changing the manner in which the program steps that use the data are executed, as in the claimed invention.*

To support the rejection under 35 USC §102(e), the Examiner relies on col. 17, lines 59-67 of the Candelore patent. However, this paragraph refers to data exchange communicated between an external memory and a cryptographic ASIC. As explained above, the data being retrieved is scrambled such a way that interception of the data will not reveal the way that the ASIC uses the data. There is no suggestion of changing the manner in which the data is processed, and therefore the Candelore patent does not anticipate the claimed invention and withdrawal of the rejection under 35 USC §102(e) is respectfully requested.

5. Rejection of Claims 1, 5-12, 21, 22, and 26-33 Under 35 USC §102(e) in view of U.S. Patent No. 6,373,946 (Johnston)

This rejection is respectfully traversed on the grounds that the Johnston patent, like the Candelore patent, does not disclose or suggest execution of commands in the operating program of a data carrier in such a way that the data processed by the corresponding commands cannot be inferred from signals detectable from outside the semiconductor chip of the data carrier. Instead, the Johnston patent merely relates to encryption of data by a semiconductor chip. There is nothing in the encryption method of Johnston to prevent an attacker from analyzing signals emitted by the chip that does the encryption in order to deduce the program steps used in the encryption and thereby reconstruct the encryption keys based on the deduced program steps and an intercepted output.

The Johnston patent concerns a particular encryption method for securing communications, involving use of a common encryption key, transmittal of the key is a secure memory using the exclusive OR operation to mask the keys. While masking of the keys using the XOR operation is a technique that is also used by the present invention (and in fact is a very basic data masking technique), however, the key masking is not used in the same way as that of the claimed invention. In Johnston, the keys are masked using exclusive OR, *and then unmasked at the receiving end so that they can be used to decrypt the transmitted communication.* **There is no modification of the decryption algorithm to compensate for the masked keys.** In the claimed invention, the masked input data is directly applied to the processing operations carried

out by the chip, and the processing operations are varied accordingly so that the **processor performs modified operations on modified input data**. As a result, only the modified input data can be inferred from the signals emitted by the chip during processing. Johnston is not at all concerned with signals emitted by the chip during execution of program steps, but only with the overall results of the execution, *i.e.*, with communications between processors. Therefore, it is respectfully submitted that the Johnston patent neither anticipates nor suggests the claimed invention, and withdrawal of the rejection under 35 USC §102(e) based on the Johnston patent is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: September 23, 2004

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500